(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06068117 A**

(43) Date of publication of application: **11.03.94**

(51) Int. Cl **G06F 15/28**

(21) Application number: **04222580**

(22) Date of filing: **21.08.92**

(71) Applicant: **NEC CORP**

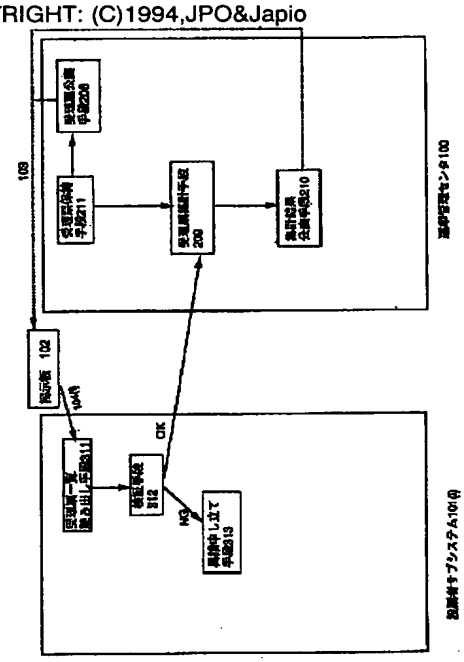
(72) Inventor: **SAKO KAZUE**

(54) **ELECTRONIC VOTING DEVICE**

(57) Abstract:

PURPOSE: To raise an objection to a case when present vote is not accepted for the vote collection while it is not known to other voters to whom the voter has voted by making all voting slips received by an election manager in public while being ciphered.

CONSTITUTION: A voter 101(i) reads a content written on a bulletin board 102 and uses a voting paper generating means to generate a voting slip composed of an approval slip, an objection slip and a voting tag along with a read format. The received slip publication means 208 of a center 100 makes all received slips and the list of tags in public. Each voter 101(i) uses a received slip list read means 311 to reads the slit of the accepted slips and the voting tags, and uses a verification means 312 to confirm that its voting is included in the list of the accepted slips and the voting tags. When not confirmed, the voter uses an objection means 313 to raise an objection. When no objection is received, a decoding key is used to decode all the accepted slips.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－68117

(43)公開日　平成６年(1994)３月11日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/28		Ｂ　7052－5Ｌ		

審査請求　有　　請求項の数３(全 13 頁)

(21)出願番号　特願平4－222580

(22)出願日　平成４年(1992)８月21日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　佐古　和恵
東京都港区芝五丁目７番１号日本電気株式会社内

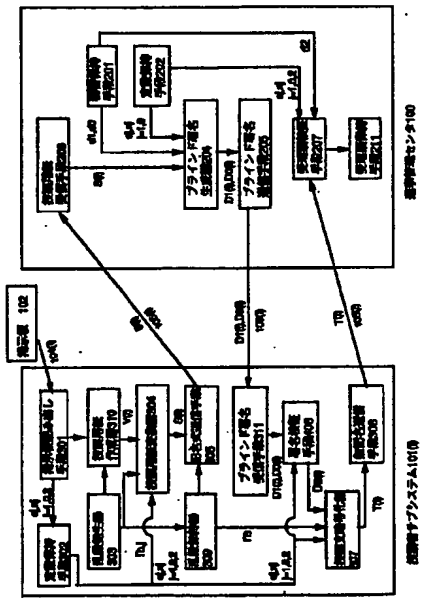
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　電子投票装置

(57)【要約】

【目的】　本発明では、投票者が自分が何に投票したかを他の投票者に知られることなく不正集計に対して異議申し立てをオープンにできる方式において、同一投票者が２つ以上の選択肢に投票することを検出でき、かつこの検出機構を第三者に悪用されない方式を提案することを目的とする。

【構成】　選択肢毎の投票用紙を、公開鍵暗号の秘密鍵で署名し、署名された投票用紙と、対応する公開鍵暗号の検証鍵（投票タグと呼ぶ）に対して選挙管理者のブラインド署名を得る投票用紙設定手段と、ブラインド署名で得た署名と投票者がつけた署名の両方をもつ投票用紙と投票タグの対を暗号化して無記名で選挙管理者に送付する投票手段と、選挙管理者は受理したすべての投票文を暗号化されたまま公開する票公開手段と、自分の投票が受理されていなければ異議申し立てを行なう票確認手段からなる。



1

【特許請求の範囲】

【請求項1】　投票者が投票用紙を変換して送出する投票用紙変換手段と、

選挙管理者が正当な有権者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、

各投票者が返信された署名文を用いて投票文に対する署名文を作成し、投票内容を暗号化して無記名で送付する投票手段と、

選挙管理者が受け取ったすべての投票文を暗号化されたまま公開する票公開手段と、

投票者が自分の投票が受理されていなければ異議申し立てを行なう受理票確認手段と、

異議申し立てがなければ、すべての票を復号化して正当な署名文が付加された投票文を集計し、公表する集計手段を有することを特徴とする電子投票装置。

【請求項2】　投票者が投票用紙を変換して送出する投票用紙変換手段と、

選挙管理者が正当な有権者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、

各投票者が返信された署名文を用いて投票文に対する署名文を作成し、署名付きの投票文を無記名で送付する投票手段と、

選挙管理者が受け取ったすべての投票文を暗号化して公開する票公開手段と、

投票者が自分の投票が受理されていなければ異議申し立てを行なう受理票確認手段と、

異議申し立てがなければ、すべての票を復号化して正当な署名文が付加された投票文を集計し、公表する集計手段を有することを特徴とする電子投票装置。

【請求項3】　投票者が投票用紙を変換して送出する投票用紙変換手段と、

選挙管理者が正当な投票者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、

各投票者が返信された署名文を用いて投票文に対する署名文を作成し、署名付きの投票文を無記名で送付する投票手段、

及び正当な署名文が付加された投票文を集計し、公表する集計手段を有する電子投票装置において、投票用紙として、各選択肢に対応する署名付き投票内容と検証鍵を含み、投票文として選択肢と検証鍵を含むことを特徴とする電子投票装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は電子ネットワーク上で有権者だけが1度だけ無記名で投票でき、投票者が自分が何に投票したかを他の投票者に知られることなく、自分の票が集計用に受理されなかった場合に異議申し立てを行なうことができる電子投票装置に関する。

【0002】

【従来の技術】電子投票方法として従来から知られているものは太田の方法がある。これは特開平1－177164号及び昭和63年電子情報通信学会春季全国大会A－294「単一の選挙管理者を用いた電子投票方式」に開示されている。この方式は投票者は乱数で変換した投票内容に対してセンタの署名を得た後、投票者側で乱数成分を取り除いたもともとの投票内容に対するセンタの署名を作成し、これを無記名でセンタに送ることにより無記名投票を実現している。各投票者は自分の投票が受理・集計されたことを、センタが発表する投票内容一覧で確認する。この方法では自分の意見を反映させた投票内容に対してのみセンタの署名を得られるので、センタがその投票内容を集計しなかった場合、自分の投票内容を公開して異議申し立てを行なわなくてはならない。

【0003】この問題を解決すべく、異議申し立てを行なう場合も、投票者が自分の投票内容を公開せずに異議申し立てを行なうために、あらかじめ投票内容に依存しない投票用紙にのみ署名をもらい、署名付きの投票用紙に自分の意見を反映させた投票内容をセンタに送るという方式が、特願平4－108069号で示された。実施例として、各有権者は賛成票・反対票及び投票タグからなる署名つき投票用紙を記名式で入手し、そのうち一方の票を投票タグと共に無記名で投票する方式が述べられている。

【0004】

【発明が解決しようとする課題】特願平4－108069号や太田の方式において、異議申し立ては集計結果判明後に行なう。したがって、賛成・反対の2値の投票を行なう場合、異議申し立て者は集計結果と反対の票に投じたと類推されるという問題点がある。本発明ではこのような投票を無効にする電子投票装置を提案する。

【0005】また、特願平4－108069号においては、投票タグに対応する賛成票・反対票を選挙管理センタが容易に偽造できるので、下記の問題が発生する。たとえば投票者Aが賛成票v_1、反対票v_0と投票タグv_1の署名を得、賛成票v_1と投票タグv_tを匿名で送付したとする。このとき、センタが反対票v'_0を偽造して、これとタグv_tを受理したと発表したとする。投票者の異議申し立て時には、投票者はv_1，v_0，v_tを公開しセンタの不正を暴くことができるが、同時に自分が賛成票に投じたことも他の投票者にわかってしまうという問題点がある。なぜならばv_tをタグとして用いた反対票に対して異議申し立てをしているからである。本発明ではこの問題点も解決する電子投票装置を提案する。

【0006】

【課題を解決するための手段】第一の発明の電子投票装置は、投票者が投票用紙を変換して送出する投票用紙変換手段と、選挙管理者が正当な有権者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、各投票者が返信された署名文を用いて投票文に対する署名文

を作成し、投票内容を暗号化して無記名で送付する投票手段と、選挙管理者が受け取ったすべての投票文を暗号化されたまま公開する票公開手段と、投票者が自分の投票が受理されていなければ異議申し立てを行なう受理票確認手段と、異議申し立てがなければ、すべての票を復号化して正当な署名文が付加された投票文を集計し、公表する集計手段を有することを特徴とする。

【０００７】第二の発明の電子投票装置は、投票者が投票用紙を変換して送出する投票用紙変換手段と、選挙管理者が正当な有権者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、各投票者が返信された署名文を用いて投票文に対する署名文を作成し、署名付きの投票文を無記名で送付する投票手段と、選挙管理者が受け取ったすべての投票文を暗号化して公開する票公開手段と、投票者が自分の投票が受理されていなければ異議申し立てを行なう受理票確認手段と、異議申し立てがなければ、すべての票を復号化して正当な署名文が付加された投票文を集計し、公表する集計手段を有することを特徴とする。

【０００８】第三の発明の電子投票装置は、投票者が投票用紙を変換して送出する投票用紙変換手段と、選挙管理者が正当な投票者の投票用紙に対して署名をし、それを投票者に返信する署名手段と、各投票者が返信された署名文を用いて投票文に対する署名文を作成し、署名付きの投票文を無記名で送付する投票手段、及び正当な署名文が付加された投票文を集計し、公表する集計手段を有する電子投票装置において、投票用紙として、各選択肢に対応する署名付き投票内容と検証鍵を含み、投票文として選択肢と検証鍵を含むことを特徴とする。

【０００９】

【実施例】つぎに、図１から図８を参照して第一、第二および第三の発明の実施例について説明する。

【００１０】本発明の電子投票装置を、図３のように、m個の投票者サブシステム１０１（1）～１０１（m）及び１つの選挙管理センタ１００が相互に安全な通信チャネル（例えばデータ回線）１０５で結ばれており、さらに選挙管理センタ１００のみが書き込み可能な掲示版で、すべての投票者サブシステムが読み出せる電子掲示版１０２が存在する場合の無記名電子投票システムに実施する例を述べる。なお、以下簡単のために選挙管理センタをセンタ、投票者サブシステムを投票者と呼ぶことにする。

【００１１】また、本実施例では簡単のために投票内容は賛成あるいは反対の２値とするが、多値にも容易に拡張できる。

【００１２】この投票システムは準備フェーズと、投票用紙設定フェーズ、投票フェーズおよび結果公表フェーズからなる。

【００１３】第一及び第二の発明は投票フェーズ及び結果公表フェーズに関する。

【００１４】まず、図1，２，４を用いて第１の発明の準備フェーズを説明する。

【００１５】本無記名電子投票システムを実施するための準備として、センタ１００は署名用の定数を設定し、検証用定数を電子掲示版１０２に掲示する。例えば、署名方式としてＲＳＡ暗号方式を用いるとする。そこで、n_1，n_0，n_2 を各々二つの素数p_1，q_1 及び p_0，q_0 並びにp_2，q_2 の積とし、e_1，e_0，e_2とd_0，d_1，d_2 を$e_i \cdot d_i = 1 \bmod (p_i - 1)(q_i - 1)$（$i=1, 0, 2$）を満たす整数とする。このときセンタは$e_i$，$n_i$（$i=1, 0, 2$）を検証用定数として設定する（ステップ11）。これらの定数を電子掲示版１０２に書き込む（ステップ１２）。今後この検証用定数e_i，n_i（$i=1, 0, 2$）は頻繁に用いられるので自分の定数保持手段２０１に書き込み容易にアクセスできるようにする（ステップ１３）。一方、d_1，d_0，d_2 は自分の秘密情報保持手段２０２に格納する（ステップ１４）。

【００１６】次に、センタ１００は投票に関する規則を定める。まず、投票対象の議題を明らかにし、１組の賛成票・反対票及びタグ票の投票フォーマットを定める。たとえば、以下のような投票フォーマットを考える。ステップ11で設定されたn_j（$j=1, 0, 2$）がそれぞれ５１２ビットであり、$n_1 < n_2$ とする。上位第１ビットから第8 ビットの排他的論理和が１のとき賛成、０のとき反対とする。次に第９ビットから、第２４９ビットには任意の整数が入れ、次の１９２ビットは、第１ビットから第５６ビットをＤＥＳ暗号の鍵、第５７ビットから第２４９ビットを平文とみなした場合の暗号文とするフォーマットとする。このように設定した５１２ビットの数字がn_1 より小さくなるようにする。また、タグ票は上位第１ビットから第８ビットをすべて０にし、第９ビットから、第２４９ビットには任意の整数が入れ、次の１９２ビットは、第１ビットから第５６ビットをＤＥＳ暗号の鍵、第５７ビットから第２４９ビットを平文とみなした場合の暗号文とするフォーマットとする。このように設定した５１２ビットの数字がn_0 より小さくなるようにする（ステップ１５）。

【００１７】次に、投票する権利のあるサブシステム（以後、有権者と呼ぶ）の名前を一覧にする（ステップ１６）。投票用紙作成及び投票の期限を設定・公表し（ステップ１７）、投票用紙作成フェーズの開始を合図する（ステップ１８）。

【００１８】以上が準備フェーズである。

【００１９】次に、投票用紙作成フェーズ、及び投票フェーズを説明するが、両フェーズとも選挙管理センタ１００は各投票者に対して同じ手順を踏むので、特定の投票者サブシステム１０１（ｉ）に対する手順を例にとって説明を続ける。

【００２０】図１に示すように無記名電子投票システム

はセンタ１００が電子掲示版１０２に定数及び投票規則を書き込む安全通信チャネル１０３、投票者１０１（ｉ）が電子掲示版１０２に書かれた内容を読み出すための安全通信チャネル１０４（ｉ）および投票者とセンタが交信するための安全通信チャネル１０５（ｉ）で構成されている。

【００２１】まず、図１を参照しながら投票者１０１（ｉ）の投票用紙作成フェーズを説明する。

【００２２】投票者１０１（ｉ）は掲示板読み出し手段３０１を用いて掲示板１０２に書かれてある内容を読み出し、定数e_j，n_j（ｊ＝１，０，２）を定数保持手段３０２に格納する一方、読み出したフォーマットに沿うよう投票用紙作成手段３１０にて賛成票$v_{1,1}$・反対票$v_{1,0}$・投票タグ$v_{0,0}$からなる投票用紙Ｖ（ｉ）を生成する。これを

$V(i)=(v_{1,1}, v_{1,0}, v_{0,0})$

と表す。なお、各賛成票・反対票及び投票タグ作成にあたってフォーマットに必要な乱数成分は乱数発生器３０３の出力を用いる。

【００２３】次に、投票用紙変換器３０４は、乱数発生器３０３の出力$r_{b,j}$と定数e_b，n_b（ｂ＝１，０）を用いて、

【００２４】

【数１】

$$S_{b,j}=v_{b,j}\cdot r_{b,j}^{e_b} \bmod n_b$$

【００２５】を（ｂ，ｊ）＝（１，０），（１，１），（０，０）のそれぞれに対して計算し、$s_{b,j}$からなるベクトルＳ（ｉ）＝（$s_{1,1}$，$s_{1,0}$，$s_{0,0}$）を出力する。また、このときの乱数発生器３０３の出力$r_{b,j}$は乱数保持器３０９に格納する。Ｓ（ｉ）を記名付き交信手段３０５が安全チャネル１０５＊を通じてセンタ１００に送信する。

【００２６】センタ１００は投票用紙受信手段２０６で受信した正当な有権者からのＳ（ｉ）を受信する。ブラインド署名生成器２０４は秘密保持手段２０１、定数保持手段２０２から読みだしたd_b及びn_bを用いて、

【００２７】

【数２】

$$D_{b,j}=s_{b,j}^{d_b} \bmod n_b$$

【００２８】を各（ｂ，ｊ）＝（１，０），（１，１），（０，０）について計算し、出力する。ブラインド署名送信手段２０５はＤ（ｉ）＝（$D_{1,0}$，$D_{1,1}$，$D_{0,0}$）を投票者１０１（ｉ）に送信する。

【００２９】投票用紙作成を行なったすべての有権者に対して署名を送信すればセンタは投票フェーズに移行することを宣言する。以上が投票用紙設定フェーズである。

【００３０】次に、投票フェーズを説明する。

【００３１】署名検証手段３０６は、ブラインド署名受信手段３１１によりセンタ１００から受信したＤ（ｉ）と、定数保持手段３０２から読み出したe_b，n_bを用いて

【００３２】

【数３】

$$s_{b,j}=d_{b,j}^{e_b} \bmod n_b$$

【００３３】が各（ｂ，ｊ）＝（１，０），（１，１），（０，０）について成立するかどうか検証する。

【００３４】確認できれば、投票暗号化器３０７は、自分の意見Ｂ（Ｂは０か１）に対して、乱数保持器３０９から読み出した整数$r_{1,B}$，$r_{0,0}$と、定数保持手段３０２から読み出したn_1，n_0，e_2を用いて、

$$t_{1,B}=((d_{1,B}/r_{1,B}) \bmod n_1)^{e_2} \bmod n_2$$

$$t_{0,0}=d_{0,0}/r_{0,0} \bmod n_0$$

を計算し、無記名送信手段３０８はＴ（ｉ）＝（$t_{1,B}$，$t_{0,0}$）を送信者名を付記せずにセンタ１００に送出する。

【００３５】センタ100 は、受信したＴ（ｉ）のうち$t_{0,0}$を読み出し

【００３６】

【数４】

$$\alpha=t_{0,0}^{d_0} \bmod n_0$$

【００３７】を計算する。αは投票者が不正をしていなければ、$v_{0,0}$に等しくなる。αがあらかじめ定められたタグのフォーマットであれば、これと同じタグが以前使われているかどうか検証する。使われていなければ、$t_{1,B}$を受理票とするとともに、使用済タグとしてαを記録する。$t_{1,B}$，αを受理票保持手段２１１に格納する。同じタグが使われていれば、無効票として受理しない。

【００３８】以上が投票フェーズである。全員の投票が終了したら、センタは結果公表フェーズへ移る。

【００３９】次に図２を用いて結果公表フェーズを説明する。

【００４０】センタ１００は受理票公表手段２０８において、受け取ったすべての受理票とそのタグの一覧を公表する。各投票者１０１（ｉ）は受理票一覧読み出し手段３１１において、受理票と投票タグの一覧を読み出し、検証手段３１２において自分の投票が票及びタグが一覧に含まれていることを確認する。確認できなければ、異議申し立て手段３１３を用いて異議申し立てを行なう。これについては後で詳細に述べる。センタはどの投票者からも異議申し立てがなければ、復号鍵d_2を用いてすべての受理票を復号化し、e_1を用いて署名を確かめる。すなわち、

【００４１】

【数５】

$$\beta=(t_{1,B}^{e_B} \bmod n_2)^{e_1} \bmod n_1$$

【００４２】が定められたフォーマットに従った正当な票になっていることを確かめる。確かめられればこの票の値に基づいて集計を行なう。確かめられない場合は無効票とする。

【００４３】全部の票が集計できれば、復号鍵とともに集計結果を公表する。各投票者は受理票を復号鍵で復号すれば公表された集計結果になることを検証できる。

【００４４】一方、検証手段３１２において自分の投票が受理されていなければ、異議申し立て手段３１３において、以下をとり行なう。

【００４５】ブラインド署名受信手段３１１にて受信し、署名検証手段306 において検証されたＤ（ｉ）と、定数保持手段３０２から読み出したe_b，n_b をおよび乱数保持手段３０９から読み出した$r_{b,j}$ を用いて

$$\gamma_{b,j} = s_{b,j} / r_{b,j} \bmod n_b$$

各（ｂ，ｊ）＝（１，０），（１，１），（０，０）について計算し、異議申し立て時に公表する。

【００４６】

【数６】

$$\gamma_{0,0}^{e_2} \bmod n_2$$

【００４７】となるｊ＝０，１のいづれもの受理票および

$\gamma_{0,0}$

のタグが公表されていないことが確認されれば、異議申し立て者の票が受理されていないと処理される。

【００４８】このように異議を申し立てれば、異議申し立て者が実際はどちらの票を投票したのかを明らかにすることなく、自分の票が受理されなかったことを証明することができる。さらに、異議申し立て時には全体の投票結果は暗号化されたままなので、投票結果に対する異議とは区別され、従来の方式の様に異議申し立て者が投票結果が不満で異議を唱えているのではないことが明らかになる。

【００４９】なお、本発明を賛成・反対両方に投票する不正投票者が存在しない場合に適用する場合には、投票タグは一切用いなくても同じ効果をもたらす。

【００５０】次に図６，７を用いて第二の発明の実施例を説明する。

【００５１】第二の発明は、第一の発明と同様、集計結果を公開する前に、暗号化された受理票を公開して、自分の投票が集計されているかどうかを見るにする。第一の発明では投票者が自分の投票内容をセンタの公開鍵で暗号していたが、第二の発明では処理能力の大きいセンタが、受理した投票を公開鍵で暗号化して公表することにする。これにより、投票者の負担軽減が見込まれる。

【００５２】上記の第一の発明の実施例と準備フェーズ、投票用紙作成フェーズは同様であるが、投票フェーズにおける投票文作成器５００と公表フェーズにおける受理票暗号化手段５０１が異なっているので差異だけ説明する。投票文作成器５００では自分の意見Ｂ（Ｂは０か１）に対して、乱数保持器３０９から読み出した整数$r_{1,B}$，$r_{0,0}$ と、定数保持手段３０２から読み出したn_1，n_0 を用いて、

$$t_{1,B} = (d_{1,B} / r_{1,B}) \bmod n_1$$

$$t_{0,0} = d_{0,0} / r_{0,0} \bmod n_0$$

を計算し、無記名送信手段３０８はＴ（ｉ）＝（$t_{1,B}$，$t_{0,0}$）を送信者名を付記せずにセンタ１００に送出する。

【００５３】センタは受理票検証手段２０７でこれの正当性を検証できれば受理票保持手段２１１に格納する。

【００５４】以上が投票フェーズである。

【００５５】公表フェーズにおいては、センタは受理票保持手段２１１に格納されている受理票をあらかじめ公開してある公開鍵e_2，n_2 を用いて暗号化し、暗号化された受理票を公表する。各投票者の検証手段３１２では、自分の票を公開鍵e_2，n_2 で暗号化したものと比較して、自分の票が受理されているか否かを調べる。

【００５６】次に図４、８を用いて第三の発明の実施例を説明する。第三の発明は主に投票用紙設定フェーズに関する。

【００５７】まず、図４を持ちいて第三の発明の準備フェーズを説明する。

【００５８】本無記名電子投票システムを実施するための準備として、センタ１００は署名用の定数を設定し、検証用定数を電子掲示版１０２に掲示する。例えば、署名方式としてＲＳＡ暗号方式を用いるとする。そこで、n_1，n_0，n_2 を各々二つの素数p_1，p_1 及びp_0，p_0 並びにp_2，p_2 の積とし、e_1，e_0，e_2とd_1，d_0，d_2 を$e_i \cdot d_i = 1 \bmod (p_i - 1)(q_i - 1)$（ｉ＝１，０，２）を満たす整数とする。このときセンタはe_i，n_i（ｉ＝１，０，２）を検証用定数として設定する（ステップ１１）。これらの定数を電子掲示版１０２に書き込む（ステップ１２）。今後この検証用定数e_i，n_i（ｉ＝１，０，２）は頻繁に用いられるので自分の定数保持手段６２１に書き込み容易にアクセスできるようにする（ステップ１３）。一方、d_1，d_0，d_2 は自分の秘密情報保持手段６２２に格納する（ステップ１４）。

【００５９】次に、センタ１００は投票に関する規則を定める。まず、投票対象の議題を明らかにし、１組の賛成票・反対票及びタグ票の投票フォーマットを定める。たとえば、以下のような投票フォーマットを考える。ステップ１１で設定されたn_1が５１２ビットであり、上位第１ビットから第８ビットの排他的論理和が１のとき賛成、０のとき反対とする。次に第９ビットから、第２４９ビットには任意の整数が入れ、次の１９２ビットは、第１ビットから第５６ビットをＤＥＳ暗号の鍵、第５７ビットから第２４９ビットを平文とみなした場合の暗号文とするフォーマットとする。このように設定した５１２ビットの数字がn_1 より小さくなるようにする

（ステップ１５）。

【００６０】次に、投票する権利のあるサブシステム（以後、有権者と呼ぶ）の名前を一覧にする（ステップ１６）。投票用紙作成及び投票の期限を設定・公表し（ステップ１７）、投票用紙作成フェーズの開始を合図する（ステップ１８）。

【００６１】以上が準備フェーズである。

【００６２】次に、投票用紙作成フェーズ、及び投票フェーズを説明するが、両フェーズとも選挙管理センタ１００は各投票者に対して同じ手順を踏むので、特定の投票者サブシステム１０１（ｉ）に対する手順を例にとって説明を続ける。

【００６３】図６に示すように無記名電子投票システムはセンタ１００が電子掲示版１０２に定数及び投票規則を書き込む安全通信チャネル１０３、投票者１０１（ｉ）が電子掲示版１０２に書かれた内容を読み出すための安全通信チャネル１０４（ｉ）および投票者とセンタが交信するための安全通信チャネル１０５（ｉ）で構成されている。

【００６４】図６を参照しながら投票者１０１（ｉ）の投票用紙作成フェーズを説明する。

【００６５】投票者１０１（ｉ）は掲示板読み出し手段６０１を用いて掲示板１０２に書かれてある内容を読み出し、定数e_j，n_j（ｊ＝１，０，２）を定数保持手段６０２に格納する。

【００６６】次に投票用紙作成手段６１０にて以下を行なう。乱数発生器６０３の出力を用いて署名用の定数を設定する。ここではＲＳＡ署名を用いるとし、署名鍵ｄ、検証鍵ｅ，ｎを定める。ここで、ｎはn_1より小さく、ｅ，ｎを連結したものがn_0より小さくなるようにする。たとえばｎを５２０ビット、ｅを１０ビット、n_0は５３０ビットなどと準備フェーズでセンタがあらかじめ決めておけばよい。

【００６７】次にフォーマットに沿ったｎより小さい賛成票$u_{1,1}$・反対票$u_{1,0}$を定め、それらの署名文

【００６８】

【数７】

$$v_{i,b}=\overline{v}_{i,b} \bmod n \quad (b=1,\ 0)$$

【００６９】を求める。投票タグ$u_{0,0}$はｅ，ｎを連結したものとする。この３組を投票用紙Ｖ（ｉ）とし、

Ｖ（ｉ）＝（$v_{1,1}$，$v_{1,0}$，$v_{0,0}$）

と表す。次に、投票用紙変換器６０４は、乱数発生器６０３の出力$r_{b,j}$と定数e_b，n_b（ｂ＝１，０）を用いて、

【００７０】

【数８】

$$s_{b,j}=v_{b,j}\cdot r_{b,j}^{e_b} \bmod n_b$$

【００７１】を（ｂ，ｊ）＝（１，０），（１，１），（０，０）のそれぞれに対して計算し、$s_{b,j}$からなるベクトルＳ（ｉ）＝（$s_{1,1}$，$s_{1,0}$，$s_{0,0}$）を出力する。また、このときの乱数発生器６０３の出力$r_{b,j}$は乱数保持器６０９に格納する。ｓ（ｉ）を記名付き交信手段６０５が安全チャネル１０５（ｉ）を通じてセンタ１００に送信する。センタ１００は投票用紙受信手段６２６で受信した正当な有権者からのｓ（ｉ）を受信する。ブラインド署名生成器６２４は秘密保持手段６２１、定数保持手段６２２みだしたd_b及びn_bを用いて、

【００７２】

【数９】

$$D_{b,j}=s_{b,j}^{d_b} \bmod n_b$$

【００７３】を各（ｂ，ｊ）＝（１，０），（１，１），（０，０）について計算し、出力する。ブラインド署名送信手段６２５はＤ（ｉ）＝（$s_{1,1}$，$s_{1,0}$，$s_{0,0}$）を投票者１０１（ｉ）に送信する。

【００７４】投票用紙作成を行なったすべての有権者に対して署名を送信すればセンタは投票フェーズに移行することを宣言する。以上が投票用紙設定フェーズである。

【００７５】次に、投票フェーズを説明する。

【００７６】署名検証手段６０６は、ブラインド署名受信手段６１１によりセンタ１００から受信したＤ（ｉ）と、定数保持手段６０２から読み出したe_b，n_bを用いて

【００７７】

【数１０】

$$s_{b,j}=D_{b,j}^{d_b} \bmod n_b$$

【００７８】が各（ｂ，ｊ）＝（１，０），（１，１），（０，０）について成立するかどうか検証する。確認できれば、投票生成器６０７は、自分の意見Ｂ（Ｂは０か１）に対して、乱数保持器６０９から読み出した整数$r_{1,B}$，$r_{0,0}$と、定数保持手段６０２から読み出したn_1，n_0を用いて、

$t_{1,B}=D_{1,B}/r_{1,B} \bmod n_1$

$t_{0,0}=D_{0,0}/r_{0,0} \bmod n_0$

を計算し、無記名送信手段６０８はＴ（ｉ）＝（$t_{1,B}$，$t_{0,0}$）を送信者名を付記せずにセンタ１００に送出する。

【００７９】センタ１００は、受信したＴ（ｉ）のうち$t_{0,0}$を読み出し

【００８０】

【数１１】

$$\alpha=t_{0,0}^{d_0} \bmod n_0$$

【００８１】を計算する。αは投票者が不正をしていなければ、$v_{0,0}$に等しくなる。αを分割してＲＳＡ検証鍵ｅ・ｎを得、これと同じ検証鍵が以前使われているかどうかチェックする。使われていなければ、$t_{1,B}$の正当性を検証する。すなわち、

【００８２】

11

【数１２】

$$t_{1,B} \bmod n$$

【００８３】が意見Ｂを表す正しいフォーマットに従った票であるかどうかを見、正しければこれを集計する。なお、同じ検証鍵が使われていれば、無効票として受理しない。

【００８４】以上が投票フェーズである。全員の投票が＊終了したら、センタは結果公表フェーズへ移り、集計結果とすべての受理票およびタグ票を公開する。

【００８５】次に、第一の発明と第三の発明を両方実施する第４の実施例について述べる。上記の第二の発明の実施例の投票文作成器６０７において、$t_{1,B}$ を定数保持手段６０２から読み出したn_1，n_2，e_2 を用いて、

$$t_{1,B} = (d_{1,B} / r_{1,B} \bmod n_1)^{e_2} \bmod n_2$$

$$t_{0,0} = d_{0,0} / r_{0,0} \bmod n_0$$

として、投票文を暗号化すればよい。この場合n_1 はn_2 より小さいものとする。あるいは、第一の発明と第三の発明を両方実施する第５の実施例として、上記の第二※※の発明の実施例の投票文作成器６０７において、$t_{1,B}$ を定数保持手段６０２から読み出したn_1，n_2，e_2 を用いて、

$$t_{1,B} = d_{1,B} / r_{1,B} \bmod n_1$$

$$t_{0,0} = (d_{0,0} / r_{0,0} \bmod n_0)^{e_2} \bmod n_2$$

と、投票タグを暗号化してもよい。この場合n_0 はn_2 より小さいものとする。

【００８６】以下は上の実施例と同様なので説明を省略する。

【００８７】また、第二の発明と第三の発明も同様にして同時に実現できる。

【００８８】図５を参照すると、いづれの実施例で述べたシステムは、通信処理機能を備えたパーソナルコンピュータ等の端末装置（TMU）４０１と、読出し専用記憶装置（ROM）４０２と、ランダムアクセス記憶装置（RAM）４０３と、乱数発生器（RNG）４０４と、シグナルプロセッサ（SP）４０６と、TMU４０１、ROM４０２、RAM４０３、RNG４０４およびSP４０６を相互に接続する共通バス４０５とから構成される。RNG４０４は乱数をSP４０６の指令により発生する。これはセンタ１００が定数設定の時に用い、また、各投票者１０１（i）の乱数発生器として用いる。ROM４０７にはセンタ１００の場合、定数e_i，n_i（i＝1，0，2）と秘密情報d_i（i＝1，0，2）を記憶している。d_i（i＝1，0，2）はTUMからブラインド署名作成の度にRAMに格納するようにしてもよい。ROM４０７には投票者サブシステム１０１（i）の場合、定数e_i，n_i（i＝1，0，2）を記憶している。ROM内に格納されたプログラムに基づいて、上述の動作を実現する。RAM４０３はこれらのステップの実行中に計算途中結果等を一時的に記憶するために用いられる。

【００８９】また、システム１００，１０１（i）は汎用電子計算機等のデータ処理装置やＩＣカードであってもよい。

【００９０】本発明は選挙や投票以外にも、無記名電子アンケートや人気調査などに適用できる。

【００９１】

【発明の効果】以上詳細に説明したように、本発明を用いれば、プライバシーを保ったまま異議申し立てができる無記名電子投票システムを実現することができる。

【図面の簡単な説明】

【図１】第一の発明の電子投票装置の一実施例を示すブロック図。

【図２】第一の発明の電子投票装置の一実施例を示すブロック図。

【図３】無記名電子投票システムを示す図。

【図４】準備フェーズの例を示す図。

【図５】センタ１００、投票者サブシステム１０１(i)の構成を示す図。

【図６】第二の発明の電子投票装置の一実施例を示すブロック図。

【図７】第二の発明の電子投票装置の一実施例を示すブロック図。

【図８】第三の発明の電子投票装置の一実施例を示すブロック図。

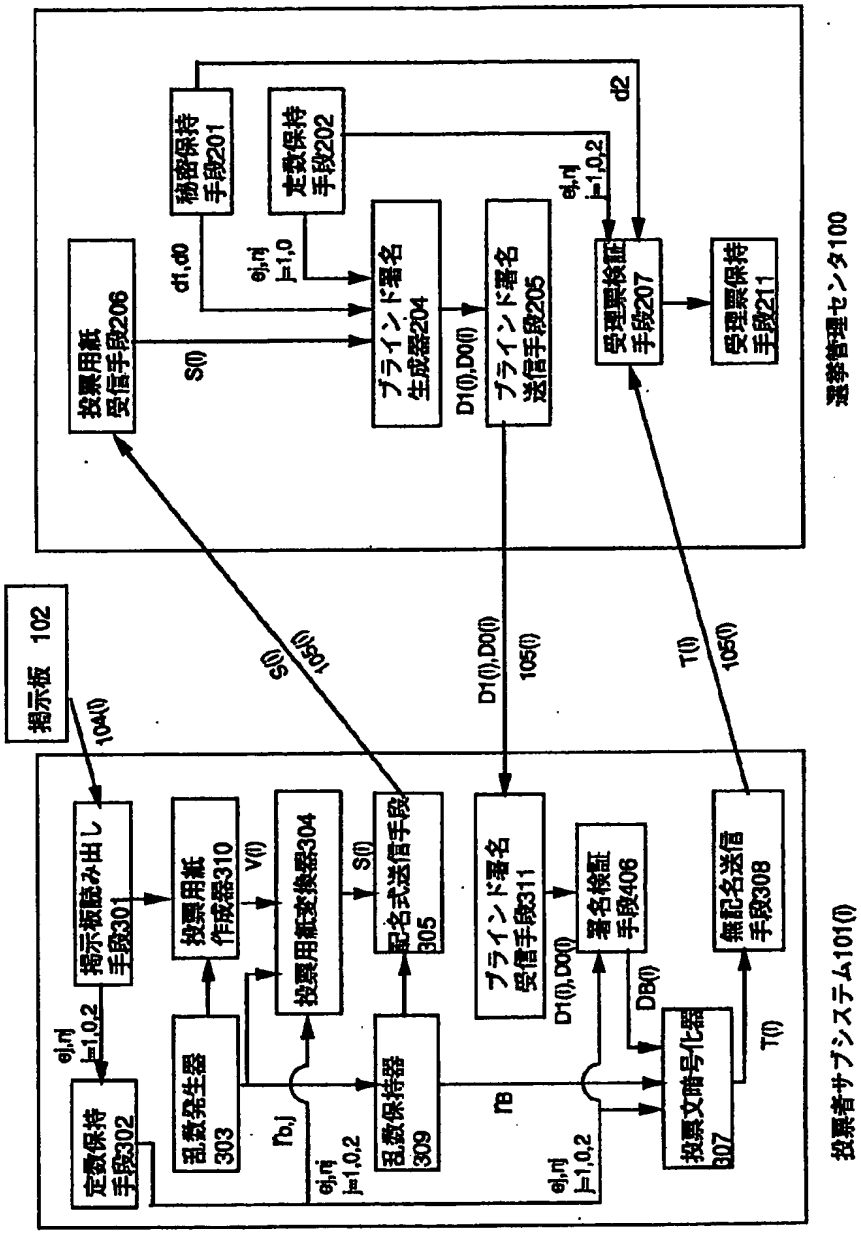
【符号の説明】

１００　選挙管理センタ

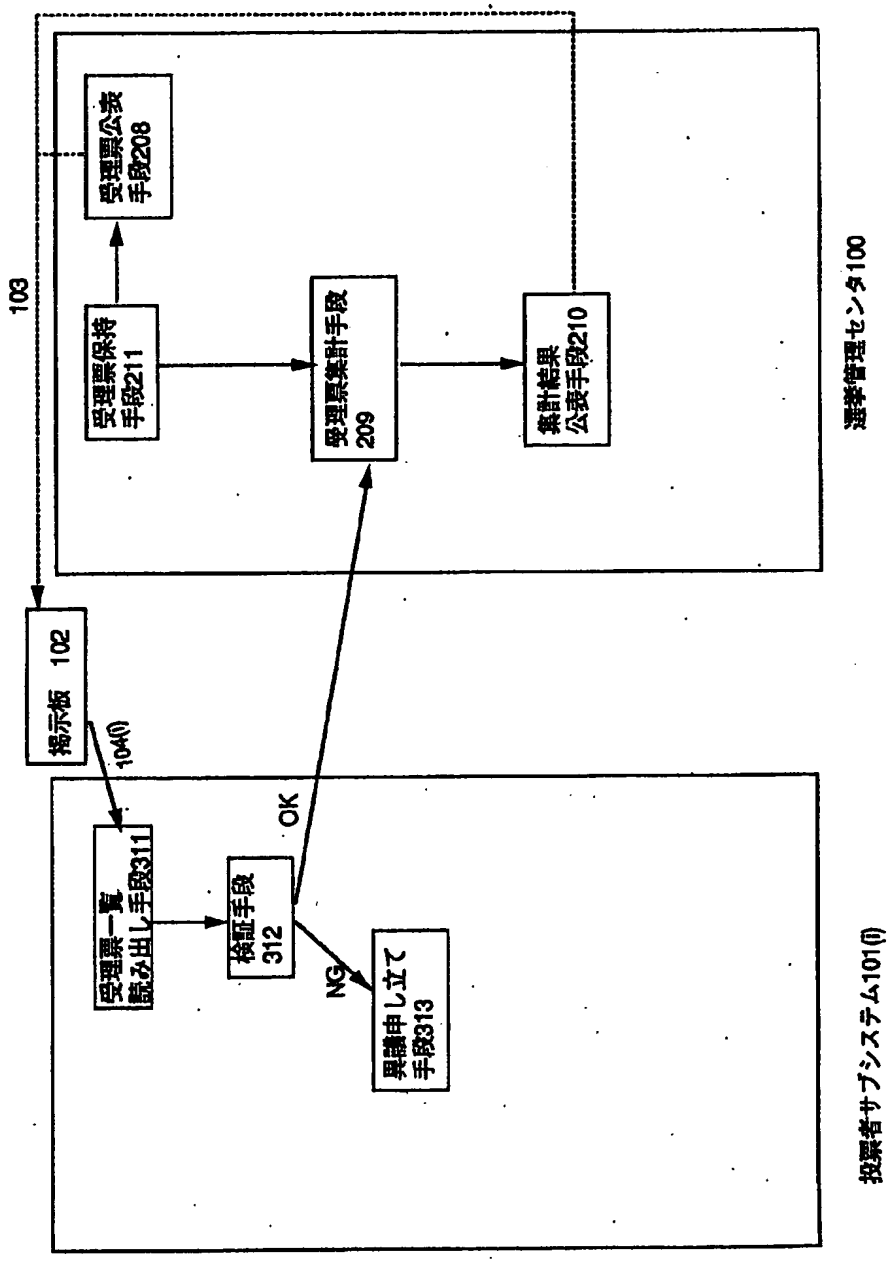
１０１（i）　投票者サブシステム

１０２　電子掲示板

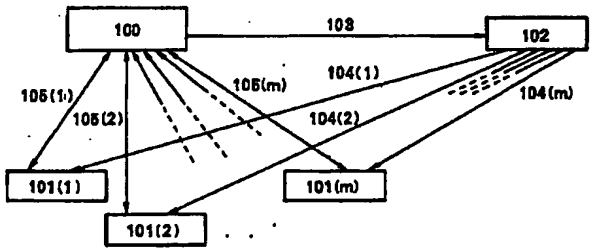
【図1】


選挙管理センタ100
秘密保持手段201
定数保持手段202
ブラインド署名生成器204
ブラインド署名送信手段205
投票用紙受信手段206
受理票検証手段207
受理票保持手段211
d1,d0
d2
S(I)
D1(I),D0(I)
T(I)
掲示板　102
104(I)
105(I)
投票者サブシステム101(I)
掲示板読み出し手段301
定数保持手段302
乱数発生器303
投票用紙変換器304
記名式送信手段305
乱数保持器309
投票用紙作成器310
ブラインド署名受信手段311
署名検証手段406
投票文暗号化器307
無記名送信手段308
V(I)
DB(I)
rB
rb,j
ej,nj j=1,0,2

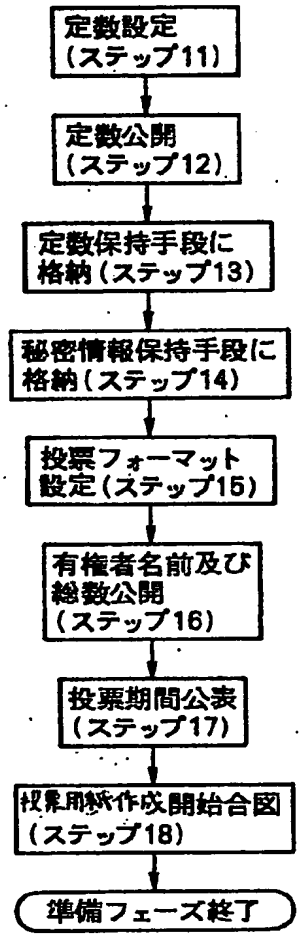
【図2】


103
受理票公表
手段208
受理票保持
手段211
受理票集計手段
209
集計結果
公表手段210
選挙管理センタ100
掲示板　102
104(i)
受理票一覧
読み出し手段311
検証手段
312
OK
NG
異議申し立て
手段313
投票者サブシステム101(i)

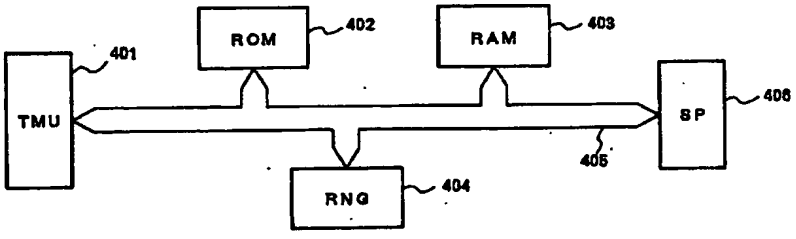
【図3】


100
103
102
105(1)
105(2)
105(m)
104(1)
104(2)
104(m)
101(1)
101(2)
101(m)

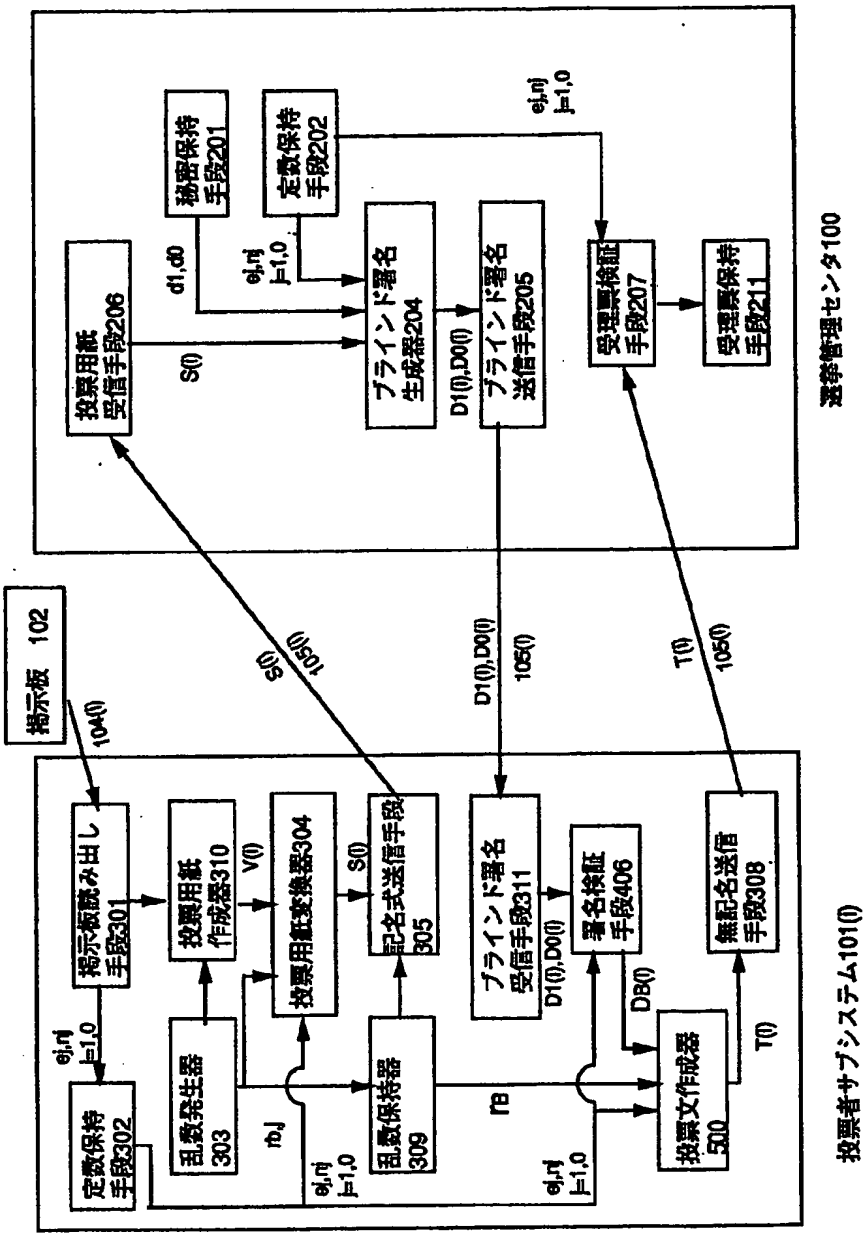
【図4】


定数設定
(ステップ11)
定数公開
(ステップ12)
定数保持手段に
格納(ステップ13)
秘密情報保持手段に
格納(ステップ14)
投票フォーマット
設定(ステップ15)
有権者名前及び
総数公開
(ステップ16)
投票期間公表
(ステップ17)
投票用紙作成開始合図
(ステップ18)
準備フェーズ終了

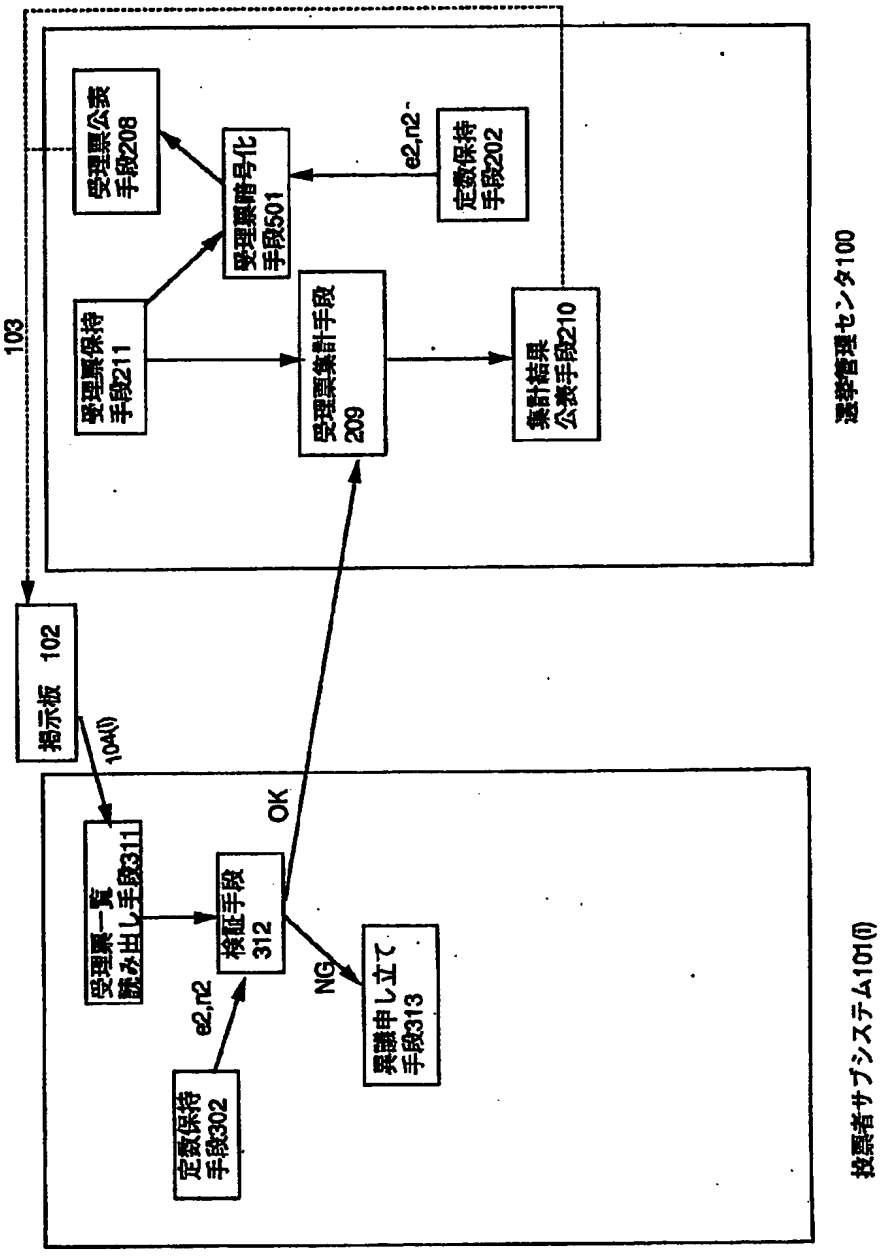
【図5】


TMU
401
ROM
402
RAM
403
RNG
404
405
SP
406

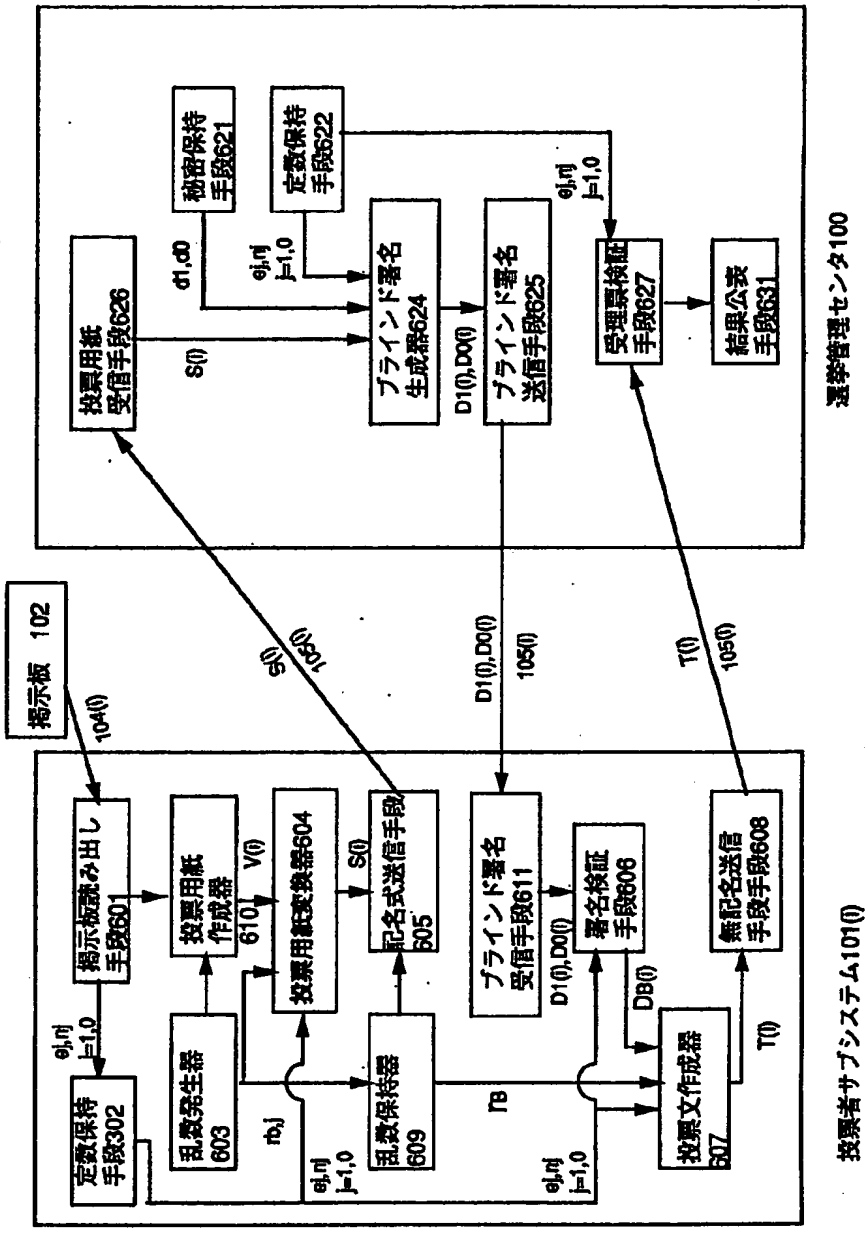
【図6】


選挙管理センタ100
秘密保持手段201
定数保持手段202
投票用紙受信手段206
ブラインド署名生成器204
ブラインド署名送信手段205
受理票検証手段207
受理票保持手段211
d1,d0
S(i)
D1(i),D0(i)
ej,nj j=1,0
投票者サブシステム101(i)
掲示板 102
104(i)
S(i) 103(i)
D1(i),D0(i) 105(i)
T(i) 105(i)
掲示板読み出し手段301
投票用紙作成器310
投票用紙変換器304
記名式送信手段305
ブラインド署名受信手段311
署名検証手段406
無記名送信手段308
定数保持手段302
乱数発生器303
乱数保持器309
投票文作成器500
V(i)
nJ
rB
DB(i)
T(i)

【図7】


受理票公表手段208
受理票暗号化手段501
e2,n2
定数保持手段202
受理票保持手段211
受理票集計手段209
集計結果公表手段210
選挙管理センタ100
103
掲示板　102
104(i)
受理票一覧読み出し手段311
検証手段312
OK
NG
異議申し立て手段313
e2,n2
定数保持手段302
投票者サブシステム101(i)

【図8】


選挙管理センタ100
投票用紙受信手段626
秘密保持手段621
定数保持手段622
ブラインド署名生成器624
ブラインド署名送信手段625
受理票検証手段627
結果公表手段631
d1,d0
ej,nj j=1,0
S(i)
D1(i),D0(i)
ej,nj j=1,0
掲示板 102
104(i)
S(i),d0(i)
D1(i),D0(i)
105(i)
T(i)
105(i)
投票者サブシステム101(i)
掲示板読み出し手段601
投票用紙作成器610
投票用紙変換器604
記名式送信手段605
ブラインド署名受信手段611
署名検証手段606
無記名送信手段608
定数保持手段302
乱数発生器603
乱数保持器609
投票文作成器607
V(i)
S(i)
D1(i),D0(i)
DB(i)
T(i)
rb,j
rB
ej,nj j=1,0
ej,nj j=1,0
ej,nj j=1,0